NOTA PÚBLICA sobre o atual debate regulatório em torno da Segurança Cibernética no Brasil

O COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br, em sua 11ª Reunião Ordinária de 2025, realizada em 14 de novembro, e no uso das atribuições que lhe confere o Decreto nº 4.829/2003, em vista de recentes debates e propostas para regular a Segurança Cibernética no país, e

CONSIDERANDO

a) Que a segurança cibernética é tema estratégico para o país, cuja solução demanda participação colaborativa dos diferentes setores da sociedade, em linha com os Princípios para a Governança e Uso da Internet no Brasil <https://www.cgi.br/resolucoes/documento/2009/003/> e os temas prioritários do CGI.br < https://www.cgi.br/resolucoes/documento/2024/049/>;

b) Que o Brasil se encontra em momento central no debate sobre cibersegurança, com a tramitação do Projeto de Lei nº 4752/2025 no Senado Federal e, ao mesmo tempo, a discussão de um Anteprojeto de Lei Geral de Cibersegurança, coordenada pelo Gabinete

de Segurança Institucional (GSI) e pelo Comitê Nacional de Cibersegurança (CNCiber);

c) Que o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) foram construídos com ampla participação social e tomando como base os princípios do CGI.br, estabelecendo marcos regulatórios equilibrados que protegem direitos fundamentais e estimulam a inovação;

d) Que as melhores práticas internacionais em cibersegurança, exemplificadas pela Diretiva NIS2 da União Europeia e pelas diretrizes da Agência da União Europeia para a Cibersegurança (ENISA), enfatizam: (i) cooperação multissetorial; (ii) descentralização na gestão de riscos; (iii) proporcionalidade das medidas; (iv) transparência e prestação de contas; e (v) proteção de direitos fundamentais;

e) Que o CGI.br compõe o Comitê Nacional de Cibersegurança (CNCiber) e participa ativamente de seus grupos e debates;

f) Que o Brasil, por meio do NIC.br, já possui o CERT.br, um Time de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional de último recurso, que atua desde 1997 com forte integração com as comunidades nacional e internacional de CSIRTs, e é internacionalmente reconhecido por sua competência e capacidade técnica;

g) Que a Estratégia Nacional de Cibersegurança (Decreto 12.573 de 2025) estabelece um conjunto de princípios que norteiam ações para todo o ecossistema nacional;

VEM A PÚBLICO

1. Solicitar que novas legislações sobre segurança cibernética no Brasil se alinhem às boas práticas internacionais, universalmente reconhecidas e adotadas por diversas entidades técnicas do campo, além de seguirem padrões e conceitos já reconhecidos, preservando a interoperabilidade jurídica e evitando-se inovações que contrariem ou confundam aspectos já consolidados globalmente;

2. Afirmar que a governança proposta para a cibersegurança no Brasil deve evitar a sobreposição de competências entre órgãos e instituições diferentes, resguardando-se os papéis já consolidados de agências setoriais, autoridades competentes e organizações técnicas, reforçando o caráter cooperativo do ecossistema de cibersegurança brasileiro;

3. Sublinhar que o estabelecimento de um Centro Nacional de Segurança deve estar de acordo com as boas práticas do campo, afastando-se qualquer tipo de função de auditoria ou sancionatória, sendo que o papel principal deste Centro deverá ser o de coordenar iniciativas, direcionando esforços e definindo metas;

4. Indicar que centros de tratamento de incidentes cibernéticos (CSIRT/ETIR) nacionais necessitam ser independentes, recebendo todos os tipos de informações sem vinculação sancionatória prévia, para evitar que o receio de punição iniba os atores de compartilharem informações críticas sobre incidentes de segurança, não podendo, portanto, o CSIRT nacional ser subordinado a um órgão regulador;

5. Alertar para a necessidade de máxima cautela no estabelecimento de regras e previsões para sanções que demandem bloqueios de aplicações, dispositivos, sítios ou outros elementos considerados no debate atual, tendo em vista o alto risco de ineficácia de medidas e de efeitos colaterais não previstos, incluindo aqueles extraterritoriais que podem vir a causar danos para países vizinhos e para a Internet como um todo;

6. Reforçar que a coesão e a consistência normativa são essenciais para que as novas políticas de cibersegurança propostas não fragilizem a Internet. Assim como na elaboração do Marco Civil da Internet foi essencial seguir diretrizes técnicas transparentes, novas legislações devem ser construídas com embasamento técnico sólido e amplo diálogo, também por meio do emprego de consultas públicas e outras modalidades correlatas quando apropriado;

7. Reiterar, assim, a disposição do CGI.br em colaborar com qualquer discussão sobre o tema, mantendo seu compromisso de atuar como espaço multissetorial e participativo para a governança da Internet no país, conforme estabelecido no Decreto nº 4.829/2003 e em linha com as provisões do Marco Civil da Internet no Brasil (Lei nº 12.965/2014, art. 24).